VZCZCXYZ0005
OO RUEHWEB

DE RUEHC #7552 2920415
ZNR UUUUU ZZH
O 161630Z OCT 09
FM SECSTATE WASHDC
TO RUEHVEN/USMISSION USOSCE IMMEDIATE 4583-4589
INFO ORG FOR SECURITY CO OP IN EUR COLLECTIVE PRIORITY
RUEAIIA/CIA WASHINGTON DC PRIORITY
RUEKJCS/SECDEF WASHINGTON DC PRIORITY
RHMFISS/JOINT STAFF WASHINGTON DC PRIORITY
RHEFDIA/DIA WASHINGTON DC PRIORITY
RHMFIUU/DTRA ALEX WASHINGTON DC PRIORITY
RUESDT/DTRA-OSES DARMSTADT GE PRIORITY
RHMFISS/HQ USCENTCOM MACDILL AFB FL PRIORITY
RHMFISS/CDR USEUCOM VAIHINGEN GE//ECJ5// PRIORITY
RHMFISS/CDRUSAREUR HEIDELBERG GE//POLAD// PRIORITY

UNCLAS STATE 107552

SENSITIVE

C O R R E C T E D C O P Y (SENSITIVE CAPTION ADDED)

SIPDIS

E.O. 12958: N/A
TAGS: EINT KCIP OSCE PARM PREL
SUBJECT: OSCE/FSC: PROPOSAL ON NATIONAL CYBERSECURITY SELF-SURVEY AND ASSESSMENT

REF: A. USOSCE 64
¶B. USOSCE 65

¶1. (U) This is an action cable. See paras 4-6.

¶2. (SBU) Summary. Based on significant interest expressed for follow up activities to the March OSCE Workshop on Enhancing Cybersecurity, Washington has developed a national cybersecurity self-survey and assessment. Washington requests that Mission begin informal discussions in the FSC leading to a proposal for a decision that would implement this self-survey and assessment. End summary.

¶3. (SBU) Per ref a, one of the recommended follow-up activities to the March workshop noted that an essential "first step" to developing cyber resiliency was a self-survey that would identify existing policies, practices, gaps, and capacities within national information infrastructures. This recommendation was made by a U.S. expert panelist and received broad support. As a result, Washington interagency cybersecurity experts have developed a self-survey and assessment for OSCE participating States. This document is based on a survey prepared for, but never used by, the United Nations International Telecommunications Union (ITU).

¶4. (SBU) Washington recommends that Mission consult with the United Kingdom in its role as FSC chair to determine interest and feasibility in tabling the self-survey and assessment as a delegation paper before the current FSC session expires. When the FSC resumes in January 2010, delegations should be positioned for serious work on the proposal in the working group, with the goal of adopting a decision by February's end.

¶5. (SBU) Washington recommends that before tabling the proposal, at the minimum, Mission seek co-sponsorship from one or all three sponsors of the March workshop (Estonia, Lithuania, Austria) and one or two additional delegations. For the latter, Mission may approach Russia or any other delegations that publicly or privately indicated interest in follow up activities to the March cybersecurity workshop.

¶6. (SBU) Mission is asked to report on the outcome of discussions with interested delegations and to advise Washington whether the timeline proposed in this guidance is reasonable.

----- Begin text of National Cybersecurity Self-Survey & Assessment -----

Delegation of the United States of America

NATIONAL CYBERSECURITY SELF-SURVEY & ASSESSMENT
DRAFT

Introduction
The March 2009 Cybersecurity Workshop in Vienna enjoyed broad participation from the members of the Organization for Security and Co-operation in Europe (OSCE). As our societies grow increasingly dependent upon information communication technologies (ICTs) to bring us together, keep us connected, and enhance our economic and social well-being, the security of these networks is increasingly a matter of security cooperation across borders. To ensure we manage to enjoy the benefits these technologies have brought us while minimizing the risks associated with their use, each nation needs to determine its cybersecurity needs and take steps to protect its critical information infrastructure protection. This self-survey is meant to help with this introspection for OSCE members.
There are two parts to this packet:
Part 1: Survey Questions is designed for each nation to attain a sense of where it stands regarding its own national cybersecurity program. It seeks to produce a snapshot of current national policy and capability, institutions and institutional relationships, relationships among government entities and between among government and private sector entities.
Part 2: Descriptions and Explanations describes the questions in part 1, including recommendations for developing and implementing a national cybersecurity program aimed at the political and management layer, and addresses the policies, institutional framework, and relationships for cybersecurity. This tool describes a model national framework against which a nation might compare its efforts.
Although this survey is intended for self-examination, the participating States may consider sharing information on best practices or identified unmet needs in order to learn from the experiences of others and offer each other assistance where possible.
NATIONAL CYBERSECURITY SELF-SURVEY & ASSESSMENT
PART 1: SURVEY QUESTIONS

¶1. Has your country conducted an assessment to determine whether and to what extent it is dependent on Information & Communications Technologies (ICT) for National Security?
a. If yes, what has been the outcome of the assessment?
b. If no, why not, and what are the obstacles of doing so?
c. If it was concluded that your country is dependent on Information & Communications Technologies (ICT) for National Security have you linked your National continuity programs to include reconstitution of ICT during crisis?

¶2. Does your country have a national cybersecurity and/or critical information infrastructure protection program?
a. If yes, who has developed said program?
b. If yes, how is your government measuring whether it is effectively implemented?
c. If no, why not, and do you have near term plans of creating one?

¶3. Has your country reviewed and updated its national laws to deal with cybercrime?
a. If yes, has there been another assessment on whether your updated national legal framework is adequate for dealing with this issue?
b. If no, what are the obstacle(s) to reviewing and updating your national laws dealing with cybercrime?

¶4. Has your country reviewed and updated its national laws to deal with terrorist use of the Internet/cyber attacks by terrorist groups?
a. If yes, has there been another assessment on whether your updated national legal framework is adequate for dealing

with this issue?
b. If no, what are the obstacle(s) to reviewing and updating your national laws dealing with terrorist use of the Internet/cyber attacks by terrorist groups?

¶5. Has your country conducted an assessment whether law enforcement has the necessary capabilities to deal effectively with cybercrime, terrorist use of the Internet/cyber attacks by terrorist groups and threats to critical infrastructure?
a. If yes, what has been the outcome of this assessment?
b. If no, will such an assessment be conducted in the near future?

¶6. Does your country co-operate bi-laterally and/or multi-laterally with other countries when dealing with cybercrime, terrorist use of the Internet/cyber attacks by terrorist groups and threats to critical infrastructure?
a. If yes, which platforms, channels and fora are utilized?
b. If no, are there plans to establish such co-operation in the near future?

¶7. Does your national government work with the private sector and academia on cybersecurity issues?
a. If yes, what are the mechanisms for interaction? Do they provide industry and academia adequate input into the process? Are they systematic or on an ad-hoc basis?
b. If no, what are the obstacle(s) to coordination with the private sector and academia?

¶8. Does your country have a national cyber incident response capability?
a. If yes, what are the relevant responsible organization(s), and what are their roles and missions?
b. If yes, do you conduct national level exercises to test processes and procedures, what organizations, (e.g Departments & Agencies) participate the most?
c. If no, what are the obstacle(s) to creating a national capability?

¶9. Does your country have an emergency warning network for cyber alerts?
a. If yes, do you publish information requirements internationally?
b. If no, what are the obstacle(s) to creating a national capability?

¶10. Has there been a national effort at outreach to the general public to create a national culture of cybersecurity?
a. If yes, what were the efforts and the results?
b. If no, what are the obstacle(s) to conducting such an effort?

¶11. Has your capital considered the role the OSCE could play in enhancing your country's cyber security, based on but not limited to the concrete recommendations and suggestions regarding the future role of the OSCE in this thematic area elaborated at the OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security held on 17-18 March 2009 in Vienna (available at FSC.DEL/92/09).
a. If yes, which of the said recommendations and suggestions have found most favor with your capital? Does your country plan to launch any pertinent initiatives in the near future?
b. If no, will your capital consider said recommendations and suggestions in the near future?

NATIONAL CYBERSECURITY SELF-SURVEY & ASSESSMENT

PART 2: DESCRIPTIONS AND EXPLANATIONS
The following describes some of the elements participating States could consider when formulating their answers to the survey questions in Part 1. This list is not meant to be definitive or comprehensive, but is only meant as guidelines.
National Strategy
Developing a National Strategy
Taking Stock of Cybersecurity Needs and Strategies
Evaluate the role of ICT in your national economy, national

security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services), and civil society. Determine the cybersecurity and critical information infrastructure protection (CIIP) risks to your economy, national security, critical infrastructures, and civil society that must be managed.
Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present, and the current management plan; note how changes in economic environment, national security priorities, and civil society needs affect these calculations.
Determine the goals of your national cybersecurity and CIIP strategy: describe the goals, current level of implementation, measures that exist to gauge its progress, its relation to other national policy objectives, and how such a strategy fits within regional and international initiatives.
Include trust building elements. A sound national strategy will include plans to:
Improve shared defense-in-depth capabilities
Improve information assurance (IA) and Computer Network Defense (CND) interoperability
Share cyber situational awareness and early warning
Link watch center-to-watch center operations and exercises
Interoperability to protect & share CND/IA information
Foster relationship with collective security institutions
Organizational Issues
Identify lead person and institution for launching cybersecurity effort. This person should have the confidence of the head of state or government, be empowered to develop the case for action, persuade key people in government of the need to improve cybersecurity, and be able to develop the necessary political support for action. A lead institution would house the lead person and should report to the head of state or government. The institution should have a mechanism to obtain advice and agreement from other government entities, as well as from the private sector and non-government entities. It need not be the operational institution for carrying out and implementing agreed upon cybersecurity actions.
Identify lead institutions for each element of the national framework. This action would include identifying leads (institutions, offices and positions) for deterring cybercrime; creating a national incident management capability; establishing public-private partnerships; and promoting a culture of cybersecurity. It may also require the identification of leads for specialized activities within an element. The lead institution for each element of the national strategy would serve as the coordinator for activities within that element. Identify lead persons and offices within each lead institution and within each significant participating agency.
Determine key stakeholders with a role in cybersecurity and CIIP and describe the role of each in the development of relevant policies and operations, including:
National government ministries or agencies, noting primary points of contact and responsibilities of each
Other government (local and regional) participants
Non-government actors, including industry, civil society, and academia
Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity

Implementing a national strategy
Organizational Issues
Identify lead institution for coordinating ongoing national efforts and mechanisms for coordination. The lead institution would have a coordinating role, but not necessarily authority over all aspects of national effort. It need not be the same as the lead institution for developing the national strategy. The lead institution for implementing a national strategy would be responsible for actions within its area of responsibility and for coordinating government wide efforts as well as for coordinating collaborative efforts among government and the

various non-government players. Identify mechanisms for coordination among the lead institution and other participants. Not all entities will participate in all cooperative arrangements and no single arrangement is likely to serve all purposes.

Establish or identify a computer security incident response team with national responsibilities (N-CSIRT). Key issues include where within government the N-CSIRT will be housed, how its operations will be funded, what functions it will handle, and how it will cooperate with other government CSIRTs, with CSIRTs from the private sector and academia, and with foreign CSIRTs, including foreign N-CSIRTs.

Identify existing expertise. An inventory of institutions, units within organizations, and individuals with relevant policy and technical expertise in government organizations, the private sector, and academia will assist in ensuring the best utilization of existing national talent and the need for training.

Identify institutions and offices with cybersecurity responsibilities. Ensure they have appropriate cooperative working arrangements between and among them for sharing of policy and technical information and the prevention, preparation, response, and recovery from an incident.

Examine infrastructure interdependencies. These include water supply and wastewater systems, energy, telecommunications, transportation, banking and finance, and emergency and government services. Mutual dependence and interconnectedness made possible by the information and communications infrastructure lead to the possibility that our infrastructures may be vulnerable in ways they never have been before. Failure to understand how disruptions to one infrastructure could cascade to others, exacerbate response and recovery efforts, or result in common cause failures leaves planners, operators, and emergency response personnel unprepared to deal effectively with the impacts of such disruptions.

Identify international and cross border counterparts. Policy and operational cooperation is also required with international and cross border entities. This cooperation must be mutually beneficial. Identify and develop cooperative relations with most relevant entities. Join relevant existing international arrangements such as the Budapest Convention.

Develop a process for sharing best practices in conjunction with the Meridian Initiative. The Meridian process aims to provide Governments worldwide with a means by which they can discuss how to work together at the policy level on critical information infrastructure protection (CIIP). An annual conference and interim activities is held each year to help build trust and establish international relations within the membership to facilitate sharing of experiences and good practices on CIIP from around the world. Participation in the Meridian process is open to all countries and aimed at senior government policy-makers.

Policies and Actions

Elaborate the case for national action. The case for national action must address several audiences; the political leadership, the business community and the public. It elaborates the importance of Critical Information Infrastructure (CII) to the nation, identifies the physical and cyber risk to the nation from failure to act, the benefits to the nation and its economy from a focused national effort to enhance cybersecurity and establish cybersecurity goals.

Elaborate a national strategy to enhance cybersecurity. This is an elaboration of the case for action and would delineate roles and responsibilities for all stakeholders in cybersecurity (government, business, other organizations and individual users), identify priorities and establish goals, timeframes and metrics. It may also place the national effort into context of international efforts or other national objectives.

Elaborate the role(s) of the N-CSIRT. The N-CSIRT would play a key role in the national effort to prepare for, detect, manage and respond to cyber incidents. An N-CSIRT could be expected to provide services and support in these areas to government entities at the national, regional and local levels; to the business community and to the general public

and individual users. Its mission could include analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding recovery efforts. It may also produce various products (publications) appropriate to its target populations and have a Critical Information Infrastructure Protection (CIIP) role.

Establish an integrated risk management process. Risk is often shared and lies outside the control of any single party. A national risk management approach supports efforts within individual infrastructures (networks and systems). Periodic assessment of the national effort is required to meet changing circumstances and to ensure continued effectiveness. A survey, exercise program, or other tools may be used as part of the effort.

Identify training requirements and how to accomplish them. Training is essential to stay abreast with developments in Information Communication Technologies (ICT), threats and vulnerabilities, and best practices in the area of cybersecurity. Such efforts may address specific needs within government as well as university or other training to meet the needs of the nation in coming years.

National Legal Frameworks

Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures, and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communication technologies, and use regional and international conventions, arrangements, and precedents were utilized in these reviews. Determine whether your nation is a party to, or plans to accede to the Budapest Convention, or plans to adopt commensurate laws.

Determine the current status of national cybercrime authorities and procedures, including legal authorities, national cybercrime units, and the level of understanding among prosecutors, judges, and legislators of cybercrime issues. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and cyberspace more generally.

Examine whether your nation participates in international efforts to combat cybercrime, such as the 24/7 Cybercrime Point of Contact Network, and determine to what extent doing so would further national cybersecurity goals.

Determine the requirements for your national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure or perpetrators reside in your national territory, but victims reside elsewhere.

Deterring Cybercrime

Organizational Issues

Within the ministry responsible for justice and law enforcement, identify the lead office for developing and implementing the Deterring Cybercrime element of the national framework. Identify a point of contact within other elements of government whose responsibilities support the Deterring Cybercrime lead. Identify non-government and private sector institutions and organizations with interest related to cybersecurity and deterring cybercrime. Develop mechanisms for policy and operational coordination and cooperation among the ministry responsible for justice and law enforcement and other government and non-government entities. Identify existing expertise and expertise requirements. Identify international and cross border counterparts.

Establish or identify national cyber crime units. The investigation and prosecution of cybercrime requires specialized equipment and personnel with specialized training and skills. The development of a national cybercrime unit to focus exclusively on cybercrime provides opportunity to maximize the return on the investments in cybersecurity equipment and personnel.

Develop cooperative relationships. There be cooperation among elements of the justice components of national authorities (police, prosecutors, judges), and cooperation among these components with national administrations addressing cybersecurity.

Cooperation with the private sector. Private sector entities are often the owners, operators and/or users of CII and may be greatly involved in protecting those resources and responding to incidents. What institutional arrangements and

procedures are in place to facilitate contact between legal/law enforcement authorities and the private sector?
Judiciary training and legislative awareness. Legislative and judiciary branches must understand the issues involved in addressing cybercrime and enhancing cybersecurity in order to achieve national goals.
Policies and actions
Conduct a base line survey of the adequacy of national substantive, procedural, and international assistance laws on cybercrime.
Identify and prioritize actions to conform the national legal infrastructure to international norms promoted by the Budapest Convention and international assistance mechanisms such as the 24/7 Cybercrime Point of Contact Network.
Creating a National Incident Management Capability
Organizational and operational Issues
Identify the agency in your government that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating government agencies; non-government cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information sharing.
Identify your national-level computer incident response capacity, including any computer incident response team with national responsibilities (N-CSIRT) and its roles and responsibilities, including existing tools and procedures for the protection of government computer networks, and existing tools and procedures for the dissemination of incident management information. Identify leadership and staff for the computer security incident response team with N-CSIRT.
N-CSIRT leadership and staff are key to the ability of the N-CSIRT to effectively carry out the roles and responsibilities assigned to it.
Identify other CSIRTs within government including those in civilian, law enforcement, defense, and intelligence agencies; points of contact; and, establish collaborative institutional and personal working relationships for consultation, cooperation, and information exchange.
Identify non-government institutions and organizations with CSIRT capabilities and expertise. Identify points of contact and collaborative working relationships for consultation, cooperation, and information exchange. Collaborative relationships that include provisions for information sharing are required.
Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.
Analysis, situational awareness and dissemination of information and products. Through its relationships with many different national and international partners, the N-CSIRT is uniquely positioned to analyze the ongoing cyber situation and to provide situational awareness to collaborating partners. To maintain that role, the N-CSIRT needs products that provide its customer base with useful information.
Develop tools and procedures for cybersecurity and the protection of cyber resources. The N-CSIRT will have a direct responsibility to assist government entities with the development and implementation of policies, procedures, methodologies, security controls and tools to protect government cyber assets, systems, networks and functions. The N-CSIRT may also play a coordinating role in efforts of the private and other sectors to develop and implement security policies and procedures.

Government - Industry Collaboration
Include industry perspectives in the development and implementation of security policy and related efforts. Involving industry will ensure utilization of its expertise and full cooperation in the final results.
Identify formal and informal venues that currently exist for government-industry collaboration in the development of cybersecurity and CIIP policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and its adequacy in achieving relevant cybersecurity and CIIP goals. Identify forums or structures

that may further be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and CIIP goals.
Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for information sharing and incident management.
Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure.
Encourage development of private sector groups from different industries to address common security interests collaboratively with government. Information infrastructures are critical to the operations of a number of industries that are themselves critical. Cooperation among such industry groups and with government is essential to enhancing cybersecurity. Encourage cooperation among interdependent industries, because cyber incidents involving one kind of infrastructure can have cascading effects and result in incidents in other kinds of infrastructure.
Establish cooperative arrangements between government and private sector for cyber incident management. Rapid identification, information exchange, and remediation can often diminish the damage cyber incidents cause. At the national level, industry-government cooperation is needed to conduct analyses, issue warnings, and coordinate response efforts.
Promoting a National Culture of Cybersecurity
Summarize actions taken and plans to develop a national culture of cybersecurity referred to in UNGA 57/239 and 58/199, including implementation of a cybersecurity plan for government-operated systems, national awareness-raising programs, outreach programs to, among others, children and individual users, and national cybersecurity and CIIP training requirements.
Implement a cybersecurity plan for government-operated systems, as outlined as the beginning of this part of the survey. Implement security awareness programs and initiatives for users of government systems and networks.
Identify lead agency, program development mechanisms, dissemination and implementation plan, and review and assessment procedures.
Develop outreach programs with business and other non-government entities. Identify lead agency, existing programs, and program development, implementation and assessment procedures. Support outreach to civil society with special attention to the needs of children and individual users.
Promote a comprehensive national awareness program so that all participants) business, the general workforce, and the general population - secure their own parts of cyber space.
Identify lead agency, existing programs, and program development, implementation and assessment procedures.
Enhance Science and Technology (S&T) and Research and Development (R&D) activities, as appropriate.
Develop awareness of specific technical issues to enhance a coordinated response to spam and malware.

------END TEXT ------
CLINTON